

Dr Artur Romaszewski

Uniwersytet Jagielloński - Collegium Medicum

Wydział Nauk o Zdrowiu

Zakład Medycznych Systemów Informacyjnych

Dr hab. med. Wojciech Trąbka

Uniwersytet Jagielloński - Collegium Medicum

Wydział Nauk o Zdrowiu

Zakład Medycznych Systemów Informacyjnych

Ochrona danych osobowych w podmiotach leczniczych i systemach informacyjnych opieki zdrowotnej – wpływ nowych, krajowych i unijnych, regulacji prawnych.

Wstęp

Problem bezpieczeństwa i poufności danych osobowych przetwarzanych w ochronie zdrowia to jedno z najważniejszych zadań przed którymi staje ochrona zdrowia w dobie kompleksowej informatyzacji.

W systemie ochrony zdrowia przetwarzane są przede wszystkim dane o stanie zdrowia pacjentów. Trzeba tym danym zapewnić bezpieczeństwo i poufność, respektując przy tym prawa pacjenta, w tym prawo dostępu do dokumentacji medycznej. Dane dotyczące stanu zdrowia są przetwarzane zarówno za zgodą, jak i bez zgody podmiotu danych. W tym drugim przypadku wynika to z przepisów prawa, uprawniających szereg instytucji do przetwarzania danych o stanie zdrowia. Taka sytuacja jest uzasadniona koniecznością uwzględnienia interesu publicznego. Dotyczy to szeregu danych związanych ze stanem zdrowia populacji¹, które umożliwiają analizowanie zachorowalności i niepełnosprawności, czynników warunkujących stan zdrowia, potrzeb w zakresie opieki zdrowotnej, zasobów opieki zdrowotnej, oferowanych usług opieki zdrowotnej i powszechnego dostępu do nich, wydatków na opiekę zdrowotną i sposobów jej finansowania oraz przyczyn zgonów.

¹ „zdrowie publiczne” należy interpretować zgodnie z definicją w rozporządzeniu (WE) nr 1338/2008 Parlamentu Europejskiego i Rady z dnia 16 grudnia 2008 r. w sprawie statystyk Wspólnoty w zakresie zdrowia publicznego oraz zdrowia i bezpieczeństwa w pracy

Problemy związane z nowymi technologiami

W wyniku rozwoju technologicznego pojawił się obszar mocy obliczeniowych i przestrzeni „wirtualnych”, oferujących całą gamę usług dotyczących przetwarzania danych, w tym o stanie zdrowia, tworzonych i zarządzanych przez podmioty gospodarcze nie mające bezpośrednio nadanego prawa do przetwarzania danych o stanie zdrowia. Mowa tutaj o chmurach obliczeniowych. Przetwarzanie może nastąpić wyłącznie po zawarciu umowy powierzenia przetwarzania danych osobowych. Umowa taka rodzi szereg problemów, głównie związanych z bezpieczeństwem danych oraz kontrolowania ich przepływu między powierzającym, a podmiotem któremu je powierzono, często usytuowanym poza obszarem Unii Europejskiej.

Warto zauważyć, że zaistniał problem tzw. danych osobistych do których należą dane o stanie zdrowia, które osoby do których należą przetwarzają w zakresie jaki uważają za wskazany. Część pacjentów zaczęło przetwarzać te dane w chmurach obliczeniowych². W myśl dotychczasowych przepisów takie dane były pozbawione ochrony. Inaczej podchodzi do tych problemów projekt Rozporządzenia UE analizowany w dalszej części tekstu. Przyjęto zasadę, że przepisy nie będą miały wprawdzie zastosowania do przetwarzania przez osobę fizyczną danych osobowych o charakterze wyłącznie osobistym, rodzinnym lub domowym, jak korespondencja i przechowywanie adresów lub sprzedaż prywatna, bez związku z działalnością zawodową lub handlową. Jednak będzie miało zastosowanie do administratorów i podmiotów, dających możliwość przetwarzania danych osobowych na potrzeby takiej działalności osobistej lub domowej³. Chodzi tutaj np. o chmury obliczeniowe dające możliwość umieszczania przez osoby fizyczne swoich danych dotyczących stanu zdrowia. Do tej pory tak powierzane dane były pozbawione ochrony.

Warto zauważyć, że wraz z postępującym procesem informatyzacji następuje zmiana podstawowego dotychczas nośnika danych o stanie zdrowia pacjenta jakim bez wątpienia

² Szerzej o tych problemach autorzy pisali w Zeszytach Naukowych nr 33 A.Romaszewski, W. Trąbka ASPEKTY PRAWNE PRZETWARZANIA DANYCH MEDYCZNYCH W CHMURACH OBLICZENIOWYCH, PROCEDURY PRZETWARZANIA DANYCH MEDYCZNYCH W ASPEKTCIE WYKORZYSTANIA CHMURY OBLICZENIOWEJ,

³ Poprawka 2Wniosek dotyczący rozporządzenia Motyw 15 - Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

była dokumentacja medyczna w postaci papierowej, na elektroniczne bazy danych gdzie gromadzone są dane o stanie zdrowia pacjentów. Wizualizacja i scalenie tak zgromadzonych danych na potrzeby pacjentów i uprawnionych podmiotów następuje tylko w razie potrzeby. Innymi słowy kompleksowa dokumentacja medyczna jest generowana z zasobów gromadzonych w bazach danych często różnych podmiotów w tylko jeżeli jest to konieczne. Proces ten spowoduje duże zmiany w przetwarzaniu danych o stanie zdrowia pacjenta.

Potrzeba nowych rozwiązań prawnych

Zasygnalizowanym wyżej i wielu innym wyzwaniom, związanym z globalną zmianą technik przetwarzania informacji musi sprostać prawo. Prawo bowiem dotyczące ochrony danych osobowych, zarówno polskie jak europejskie, zostało stworzone wiele lat temu, kiedy większość z zasygnalizowanych problemów jeszcze nie istniała. W Unii Europejskiej od lat obowiązuje Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady WE⁴, a w Polsce, w dużej mierze oparta o założenia tej dyrektywy, ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych⁵. Dyrektywa zawiera definicje podstawowych terminów odnoszących się do problematyki ochrony danych osobowych, ustala zasady zbierania, gromadzenia, przechowywania i udostępniania danych osobowych. Założenia dyrektywy wdrażały do swoich systemów prawnych państwa członkowskie Unii Europejskiej. Przykładem jest polska ustawa regulująca ochronę danych osobowych⁶. Ponieważ kraje członkowskie UE wdrażały postanowienia Dyrektywy w sposób jaki uznały za właściwy, doprowadziło to do różnic w regulacjach dotyczących danych osobowych w prawie poszczególnych krajów członkowskich. Postanowiono zmienić tą sytuację wprowadzając jeden akt prawny regulujący kompleksowo problematykę ochrony danych osobowych na obszarze całej Unii w taki sam sposób, by wyeliminować problemy związane z implementacją formy prawnej dyrektywy do prawa krajowego. W 2012 przygotowano projekt Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych⁷ – General Data Protection Regulation. Rozporządzenie⁸ to akt prawny, który

4 DYREKTYWA 95/46/WE PARLAMENTU EUROPEJSKIEGO I RADY

z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych

5 Dz. U. 1997 nr 133 poz. 883

6 Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych Dz. U. z 2014 poz. 1182

7 ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)

obowiązuje bezpośrednio w krajach członkowskich. Oznacza to, że Sejm nie będzie musiał uchylać żadnych dodatkowych ustaw ani innych aktów prawnych – nowe prawo będzie bezpośrednio wiązało podmioty, które przetwarzają dane.

Twórcy projektu wskazują na to, że przyświecały im dwa cele:

- wzmocnienia prawa do prywatności w Internecie i
- nadania impulsu gospodarce cyfrowej w Europie.

Przyjęto zasadę, jeden kontynent jedno prawo – tak Komisja Europejska reklamuje nowe przepisy w ogłoszeniu prasowym towarzyszącym ogłoszeniu projektu rozporządzenia⁹

Uznano, że Europejskie firmy nie mogą przestrzegać norm bardziej rygorystycznych niż ich konkurenci, mający swoją siedzibę poza UE, ale prowadzący działalność gospodarczą na jej obszarze. Aby zrealizować to założenie przewidziano dla ochrony danych na terenie UE formę zunifikowanego rozporządzenia.

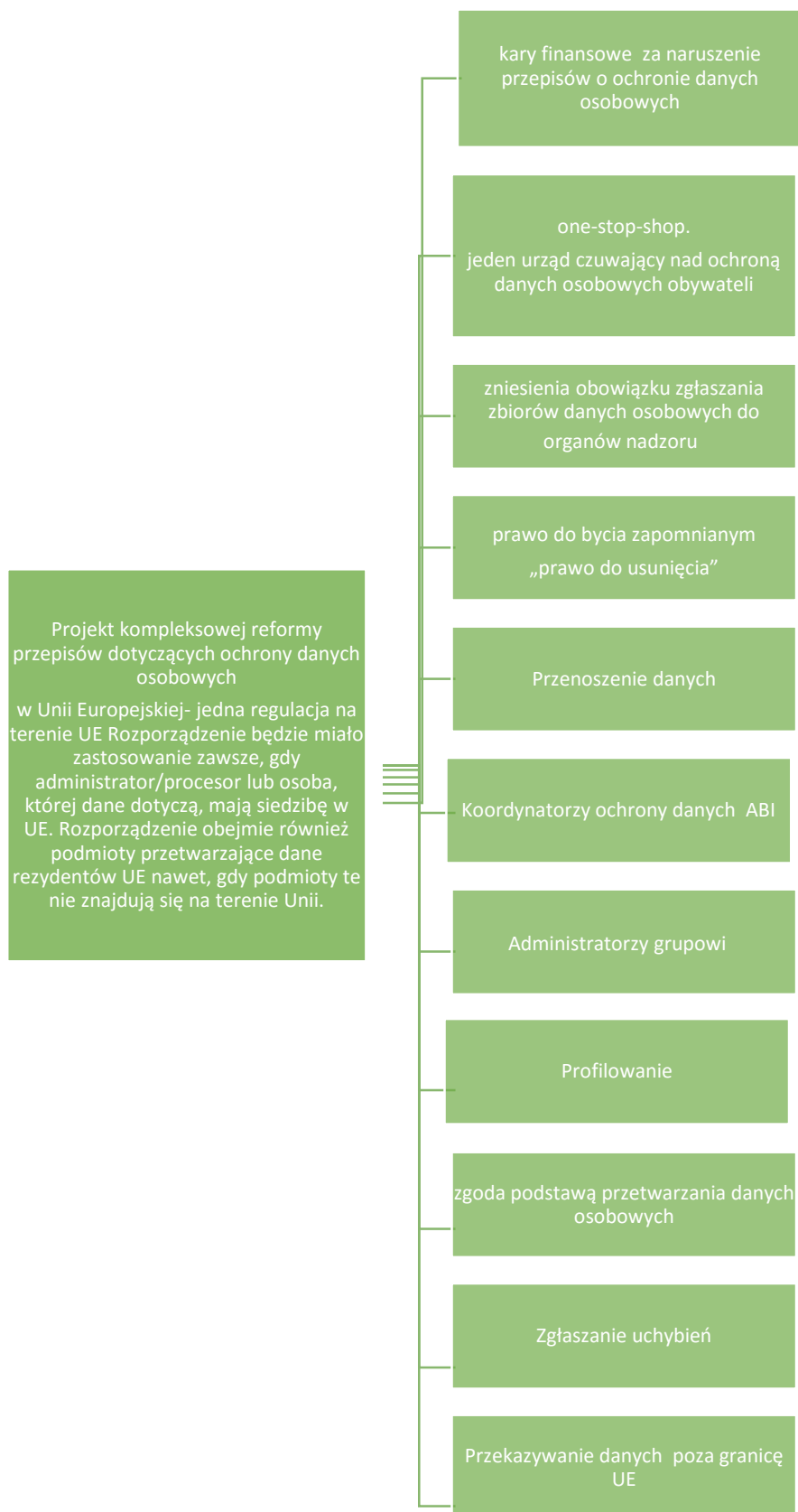
Na Rysunku 1 przedstawiono najważniejsze problemy związane z ochroną danych osobowych, które zostaną uregulowane na terenie Unii Europejskiej wraz z wejściem w życie rozporządzenia. W artykule autorzy spróbują omówić te z nich, które będą miały duży wpływ na obszar ochrony zdrowia.

W odrębnych artykułach omówiona zostanie problematyka nowych obowiązków administratorów danych oraz wprowadzenia do podmiotów świadczących usługi zdrowotne Administratorów Bezpieczeństwa Informacji¹⁰.

8 Strona Unii Europejskiej - Rozporządzenie jest wiążącym aktem prawnym. Musi być stosowane w całości na całym obszarze UE. http://europa.eu/eu-law/decision-making/legal-acts/index_pl.htm

⁹Komisja Europejska Memo http://europa.eu/rapid/press-release_MEMO-14-186_pl.htm

¹⁰A. Romaszewski W. Trąbka Administrator Bezpieczeństwa Informacji w podmiotach leczniczych w świetle ustawy o ochronie danych i Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych



Rysunek 1. najważniejsze problemy związane z ochroną danych osobowych podlegające regulacji Rozporządzenia UE

Ochrona zdrowia to bardzo ważna dziedzina życia społeczno-gospodarczego każdego państwa. Przetwarza się tutaj cały szereg danych osobowych, nie tylko takich, które dotyczą samego procesu udzielania świadczeń zdrowotnych, ale również m.in. dane pracowników, osób świadczących usługi na podstawie umów cywilnoprawnych, dane dostawców materiałów i towarów. Stąd należy kilka uwag poświęcić również aspektom rozporządzenia o charakterze ogólnym. Przede wszystkim należy zacząć od definicji danych osobowych.

Dane osobowe i dane dotyczące zdrowia

Definicja danych osobowych, która została zamieszczona w tekście rozporządzenia jest zbliżona do tej, która obecnie znajduje się w obowiązującej w Polsce ustawie o ochronie danych. Dane osobowe oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („podmiotu danych”); osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, w szczególności za pomocą takich danych identyfikujących, jak imię i nazwisko, numer identyfikacyjny, miejsce pobytu, niepowtarzalny identyfikator lub co najmniej jeden szczególny czynnik określający tożsamość fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową czy społeczną lub płciową tej osoby;

Tak więc danymi osobowymi są zarówno dane dotyczące:

- zidentyfikowanej osoby fizycznej jak i
- takie na podstawie których można osobę fizyczną, zidentyfikować, bezpośrednio lub pośrednio, za pomocą wszelkich środków, które z rozsądnym prawdopodobieństwem mogą być użyte przez administratora lub inną osobę fizyczną bądź prawną, szczególnie przez odniesienie do numeru identyfikacyjnego, danych dotyczących lokalizacji, identyfikatora online lub przynajmniej jednego czynnika charakterystycznego dla fizycznej, fizjologicznej, genetycznej, umysłowej, ekonomicznej, kulturowej lub społecznej tożsamości tej osoby. Osoby fizyczne korzystające z usług internetowych można identyfikować na podstawie identyfikatorów internetowych, które znajdują się w urządzeniach, aplikacjach, narzędziach i protokołach, takich jak adresy IP lub identyfikatory plików cookie. Mogą one zostawiać ślady, które, w połączeniu z unikatowymi identyfikatorami

i innymi informacjami uzyskanymi przez serwery, mogą być wykorzystywane do tworzenia profili poszczególnych osób i ich identyfikacji. W wyniku tego należy rozważyć, odrębnie dla poszczególnych przypadków i przy uwzględnieniu rozwoju technologicznego, czy numery identyfikacyjne, dane dotyczące lokalizacji, identyfikatory internetowe lub inne szczególne czynniki jako takie muszą być uważane za dane osobowe w każdych okolicznościach.

Zdefiniowano pojęcia związane z danymi medycznymi :

- „dane dotyczące zdrowia” oznaczają wszelkie dane osobowe związane ze zdrowiem fizycznym lub psychicznym danej osoby lub ze świadczeniem usług zdrowotnych na jej rzecz;
- „dane genetyczne” to dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, wynikające z analizy próbki biologicznej danej osoby, w szczególności z analizy chromosomów, kwasu dezoksyrybonukleinowego (DNA) lub kwasu rybonukleinowego (RNA) lub z analizy wszelkich innych elementów umożliwiających pozyskanie równoważnych informacji ;
- „dane pseudonimiczne” oznaczające dane osobowe, których nie można przypisać konkretnemu podmiotowi danych bez użycia dodatkowych informacji, o ile takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie podmiotowi danych;

Wyodrębniono również kategorię danych mających szeroki zastosowanie w ochronie zdrowia :

„dane zaszyfrowane” oznaczające dane osobowe, które za pomocą technologicznych środków ochrony stały się nieczytelne dla każdego, kto nie jest uprawniony do dostępu do nich;

„dane biometryczne” oznaczają wszelkie dane osobowe dotyczące cech fizycznych, fizjologicznych i behawioralnych danej osoby, które umożliwiają jej precyzyjną identyfikację, takie jak wizerunek twarzy lub dane daktyloskopijne ¹¹;

11 Poprawka 98 Wniosek dotyczący rozporządzenia Artykuł 4 - Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

Dane o stanie zdrowia należą do grupy tzw. danych wrażliwych. Bez wyraźnej zgody podmiotu, którego dotyczą nie powinny być one przetwarzane. Odstępstwa od zakazu przetwarzania danych wrażliwych wynikają z przepisów. Ich przetwarzanie odbywa się na podstawie przepisów prawa przy zapewnieniu odpowiednich gwarancji praw osób których dane dotyczą oraz jeżeli przemawia za tym interes publiczny.

Określono zakres danych osobowych dotyczących stanu zdrowia. Jest to o tyle istotne, że w prawie polskim brakuje tego typu definicji. (tabela 1)

Zakres danych osobowych dotyczących stanu zdrowia
<ul style="list-style-type: none"> wszelkie dane dotyczące stanu zdrowia podmiotu danych,
<ul style="list-style-type: none"> informacje na temat rejestracji osoby fizycznej w celu świadczenia usług zdrowotnych;
<ul style="list-style-type: none"> informacje o płatnościach danej osoby fizycznej za opiekę zdrowotną lub kwalifikowaniu się danej osoby do korzystania z opieki zdrowotnej;
<ul style="list-style-type: none"> numer, symbol lub oznaczenie przypisane danej osobie wyłącznie w celu identyfikowania jej dla potrzeb świadczenia opieki zdrowotnej;
<ul style="list-style-type: none"> wszelkie informacje na temat tej osoby zebrane w okresie świadczenia opieki zdrowotnej na jej rzecz; informacje pochodzące z badań laboratoryjnych lub lekarskich dotyczących części ciała lub płynów ustrojowych, w tym próbek biologicznych;
<ul style="list-style-type: none"> informacje umożliwiające identyfikację osoby świadczącej usługi opieki zdrowotnej na rzecz danego pacjenta oraz wszelkie informacje np. na temat choroby, niepełnosprawności, ryzyka choroby, historii medycznej, leczenia klinicznego lub aktualnego stanu fizjologicznego lub biomedycznego podmiotu danych, niezależnie od ich źródła, którym może być np. lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne, badanie diagnostyczne <i>in vitro</i>¹².

Tabela 1 Zakres danych osobowych dotyczących stanu zdrowia, opracowanie własne na podstawie tekstu Rozporządzenia

¹² Akapit 26 Wniosek ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)

Warunki przetwarzania danych osobowych dotyczących zdrowia

Przetwarzanie danych osobowych dotyczących zdrowia musi odbywać się na podstawie prawa Unii lub prawa państwa członkowskiego, które przewiduje odpowiednie, spójne i konkretne środki mające na celu zabezpieczenie interesów oraz praw podstawowych podmiotu danych, o ile są niezbędne:

a) dla celów medycyny prewencyjnej lub medycyny pracy, diagnostyki medycznej, opieki lub leczenia lub zarządzania opieką zdrowotną, w przypadkach, gdy dane te są przetwarzane przez pracownika służby zdrowia podlegającego obowiązkowi zachowania tajemnicy zawodowej lub przez inną osobę również podlegającą równoważnemu obowiązkowi zachowania poufności na podstawie prawa państwa członkowskiego lub przepisów ustanowionych przez właściwe organy krajowe; lub

b) ze względu na interes publiczny w dziedzinie zdrowia publicznego, taki jak ochrona przed poważnymi transgranicznymi zagrożeniami dla zdrowia lub zapewnienie wysokich standardów jakości i bezpieczeństwa, między innymi w przypadku produktów leczniczych lub wyrobów medycznych, oraz jeżeli dane te są przetwarzane przez osobę podlegającą obowiązkowi zachowania poufności; lub

c) ze względu na inne przesłanki z zakresu interesu publicznego w takich obszarach jak ochrona socjalna, szczególnie w celu zapewnienia odpowiedniej jakości i efektywności ekonomicznej procedur stosowanych do rozstrzygania roszczeń w sprawie świadczeń i usług w ramach systemu ubezpieczeń zdrowotnych i świadczenia usług zdrowotnych. Przetwarzanie danych osobowych dotyczących zdrowia ze względu na interes publiczny nie może skutkować przetwarzaniem danych osobowych do innych celów, chyba że odbywa się to za zgodą podmiotu danych lub na podstawie prawa Unii bądź państwa członkowskiego.

Gdy cele powyższe można osiągnąć bez wykorzystywania danych osobowych, tego rodzaju danych nie wykorzystuje do takich celów, chyba że opiera się to na zgodzie podmiotu danych lub prawie państwa członkowskiego.

Przyjęto zasadę, że przetwarzanie danych osobowych dotyczących zdrowia, niezbędne do celów dokumentacji, statystyki lub badań naukowych, jest dopuszczalne wyłącznie za zgodą podmiotu danych.

Gdy wymagana jest zgoda podmiotu danych na przetwarzanie danych medycznych wyłącznie do związanych ze zdrowiem publicznym celów badań naukowych, zgoda może być

udzielona na jedno lub więcej konkretnych i podobnych badań. Podmiot danych może jednak wycofać zgodę w dowolnej chwili.

Przepisy państw członkowskich mogą obejmować odstępstwa od wymogu udzielenia zgody na przetwarzanie danych osobowych do celów badań naukowych, w odniesieniu do badań naukowych, które służą istotnemu interesowi publicznemu, o ile takie badania naukowe nie mogą zostać przeprowadzone inaczej.

W sytuacjach, gdy wymaga się, by podmiot danych wydał zgodę na przetwarzanie danych medycznych wyłącznie w celu badania zdrowia publicznego, może on mieć możliwość wydania ogólnej zgody na cele badań epidemiologicznych, translacyjnych i klinicznych.

Dane osobowe przetwarzane do celów badań naukowych, powinny być zanonimizowane lub, jeśli ich anonimizacja jest niemożliwa, opatrzone pseudonimem z wykorzystaniem najwyższych standardów technicznych, przy czym podejmuje się wszelkie niezbędne działania w celu zapobieżenia nieobjętej gwarancjami ponownej identyfikacji podmiotów danych. Podmiot danych ma jednak prawo do wyrażenia sprzeciwu w dowolnej chwili.

Dane osobowe mogą być przetwarzane do celów dokumentacji, statystyki lub badań naukowych jedynie wtedy, gdy:

- nie można ich inaczej osiągnąć przez przetwarzanie danych, które nie umożliwia lub przestaje umożliwiać identyfikację osoby, której dane dotyczą;
- dane umożliwiające przypisanie informacji do zidentyfikowanego podmiotu danych lub do zidentyfikowania, są przechowywane oddzielnie od innych informacji zgodnie z najwyższymi standardami technicznymi, przy czym przyjmuje się wszelkie niezbędne środki w celu zapobieżenia nieobjętej gwarancjami ponownej identyfikacji podmiotów danych.¹³

Przewidziano również, że Komisja w celu dalszego określenia innych przesłanek zakresu interesu publicznego w obszarze zdrowia publicznego, będzie mogła przyjmować akty delegowane¹⁴

13 Poprawka 194Wniosek dotyczący rozporządzenia Artykuł 83 Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

14 weszły w życie 1 grudnia 2009 r. Akty mają na celu uzupełnienie przepisów znajdujących

Ogólne zasady przetwarzania danych osobowych

Przyjęto również ogólne zasady którymi należy się kierować przy przetwarzaniu danych osobowych. Przedstawiono je w tabeli 2

Zasady dotyczące przetwarzania danych osobowych¹⁵	
zgodność z prawem, uczciwość i przejrzystość	Dane osobowe są przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty w odniesieniu do podmiotu danych
zasada celowości	Dane osobowe są zbierane w konkretnych, bezpośrednich i zgodnych z prawem celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
minimalizacja danych	Prawidłowe, właściwe i ograniczone do minimum niezbędnego w odniesieniu do celów, do których dane są przetwarzane; dane te są przetwarzane przez okres, w którym tych celów nie można spełnić, przetwarzając informacje, które nie obejmują danych osobowych.
ścisłość	Dane osobowe powinny być ścisłe i, w razie konieczności, aktualizowane; należy podjąć wszelkie zasadne działania, by zapewnić niezwłoczne usunięcie lub poprawienie nieścisłych danych osobowych, z uwzględnieniem celów ich przetwarzania
minimalizacja przechowywania	- Dane osobowe powinny być przechowywane w formie umożliwiającej bezpośrednią lub pośrednią identyfikację podmiotów danych przez czas nie dłuższy niż jest to konieczne do celów, dla których dane są przetwarzane; - dane osobowe mogą być przechowywane

się w aktach legislacyjnych (rozporządzeniach, dyrektywach, decyzjach). Ustawodawcy mogą powierzyć Komisji Europejskiej uszczegółowienie lub poprawienie –co oznacza decydowanie- w stosunku do pewnych mniej istotnych elementów prawa UE bądź prawa ramowego dzięki uprawnieniom do delegowania. Akty delegowane są nadrzędne w stosunku do ustaw i konstytucji narodowych, mimo że uchwalane są w instytucji, w której nie są reprezentowane wszystkie państwa członkowskie.

<http://pl.euabc.com/word/271> <http://pl.euabc.com/word/271>;

https://www.mir.gov.pl/rozwoj_regionalny/Polityka_regionalna/Documents/Akty_delegowane.pdf

15 Poprawka 99 Wniosek dotyczący rozporządzenia Artykuł 5 Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

	przez czas dłuższy pod warunkiem, że będą przetwarzane wyłącznie do celów dokumentacji, statystyki lub badań naukowych lub archiwizacji pod warunkiem prowadzenia okresowej kontroli konieczności dalszego ich przechowywania, a także pod warunkiem, że w stosownych przypadkach przyjęte zostaną techniczne i organizacyjne środki służące ograniczeniu dostępu do danych wyłącznie do tych celów.
Skuteczność	Przetwarzanie danych musi być wykonywane w taki sposób, który skutecznie umożliwia podmiotowi danych wykonywanie jego praw
integralność	Dane osobowe powinny być przetwarzane w sposób zabezpieczający przed niedozwolonym lub nielegalnym przetwarzaniem i przypadkową utratą, zniszczeniem lub uszkodzeniem, z wykorzystaniem odpowiednich środków technicznych i organizacyjnych
odpowiedzialność	przetwarzane pod nadzorem i na odpowiedzialność administratora, który zapewnia i jest w stanie wykazać zgodność z przepisami niniejszego rozporządzenia

Tabela 2 Zasady dotyczące przetwarzania danych osobowych. Opracowanie własne na podstawie Rozporządzenia

Przetwarzanie danych osobowych jest zgodne z prawem, o ile ma zastosowanie co najmniej jedna z poniższych przesłanek:

- ✓ podmiot danych wyraził zgodę na przetwarzanie swoich danych osobowych do jednego lub większej liczby konkretnych celów;
- ✓ przetwarzanie danych jest konieczne do wykonania umowy, której stroną jest podmiot danych, lub w celu podjęcia działań na żądanie podmiotu danych przed zawarciem umowy;
- ✓ przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze; - musi to wynikać z prawa danego kraju UE,

- ✓ przetwarzanie jest konieczne w celu ochrony żywotnych interesów podmiotów danych;
- ✓ przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub wykonania władzy publicznej powierzonej administratorowi;- - musi to wynikać z prawa danego kraju UE
- ✓ przetwarzanie jest konieczne dla celów wynikających z uzasadnionych interesów realizowanych przez administratora

Prawo państwa członkowskiego musi realizować cel leżący w interesie publicznym lub musi być konieczne do ochrony praw i wolności innych osób, respektować istotę prawa do ochrony danych osobowych i być proporcjonalne do wyznaczonego słusznego celu.

W granicach rozporządzenia UE prawo państwa członkowskiego może przewidywać szczegóły dotyczące legalności przetwarzania danych, szczególnie w kwestiach takich jak administratorzy danych, cele przetwarzania i zasada celowości, charakter danych i podmiotów danych, środki i procedury dotyczące przetwarzania, odbiorcy oraz okres przechowywania.

Wszelkie operacje przetwarzania danych osobowych powinny być zgodne z prawem, prowadzone rzetelnie i uczciwie wobec zainteresowanych osób. Dane osobowe powinny być przetwarzane tylko wówczas, gdy celu przetwarzania nie można osiągnąć innymi środkami. Należy podjąć wszelkie stosowne kroki gwarantujące poprawienie lub usunięcie nieścisłych danych osobowych. Aby uniknąć przechowywania danych przez czas dłuższy niż jest to konieczne, administrator powinien ustalić termin usuwania danych lub okresowego przeglądu.

Literatura

1. Rozporządzenie (WE) nr 1338/2008 Parlamentu Europejskiego i Rady z dnia 16 grudnia 2008 r. w sprawie statystyk Wspólnoty w zakresie zdrowia publicznego oraz zdrowia i bezpieczeństwa w pracy
2. Zeszytach Naukowych nr 33 Wyższa Szkoła Zarządzania i Bankowości A. Romaszewski, W. Trąbka ASPEKTY PRAWNE PRZETWARZANIA DANYCH MEDYCZNYCH W CHMURACH OBLICZENIOWYCH, PROCEDURY PRZETWARZANIA DANYCH MEDYCZNYCH W ASPEKCIE WYKORZYSTANIA CHMURY OBLICZENIOWEJ,

3. DYREKTYWA 95/46/WE PARLAMENTU EUROPEJSKIEGO I RADY z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych
4. ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)
5. Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))
6. Romaszewski W. Trąbka Administrator Bezpieczeństwa Informacji w podmiotach leczniczych w świetle ustawy o ochronie danych i Rozporządzenia Parlamentu Europejskiego I Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych
7. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. 1997 nr 133 poz. 883 Strona Unii Europejskiej http://europa.eu/eu-law/decision-making/legal-acts/index_pl.htm
8. Komisja Europejska Memo http://europa.eu/rapid/press-release_MEMO-14-186_pl.htm
9. J.Bardadyn Kiedy (ostatecznie!) i jak UE zreformuje prawo ochrony danych osobowych? <http://blog-daneosobowe.pl/ue-ostatecznie-zreformuje-prawo-ochronie-danych-osobowych-beda-kluczowe-zalozenia/>
10. M. Chmielecki UNIJNA REFORMA PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH - INFORMACJE OGÓLNE [e-ochronadanych.pl](http://www.e-ochronadanych.pl) <http://www.e-ochronadanych.pl/regulamin.php>
11. M. Cwener PROPOZYCJE ZMIAN W ZAKRESIE PRZEPISÓW DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH – CZ. I; ii OGÓLNE [e-ochronadanych.pl](http://www.e-ochronadanych.pl) <http://www.e-ochronadanych.pl/regulamin.php>
12. K. Szymielewicz Półprzepuszczalny standard ochrony danych <https://panoptykon.org/wiadomosc/polprzepuszczalny-standard-ochrony-danych>
13. K.Witkowska Reforma ochrony danych osobowych - nowe obowiązki, nowe korzyści <https://www.portalodo.com/entry/reforma-ochrony-danych-osobowych-nowe-obowiazki-nowe-korzysci>.
14. P. Wierzbicki Jest szansa na unijne rozporządzenie o ochronie danych (2014.02.11) Obserwator Konstytucyjny <http://www.obserwatorkonstytucyjny.pl/debaty/jest-szansa-na-unijne-rozporzadzenie-o-ochronie-danych/>

Streszczenie

W systemie ochrony zdrowia przetwarzane są przede wszystkim dane o stanie zdrowia pacjentów. Trzeba tym danym zapewnić bezpieczeństwo i poufność, respektując przy tym

prawa pacjenta, w tym prawo dostępu do dokumentacji medycznej. Wprowadzenie nowych technologii, dokumentacji elektronicznej, teletransmisji, przetwarzania w chmurach obliczeniowych, a także globalizacja dostępu do tych danych wymagała wprowadzenia tak na poziomie krajowym jak i UE nowych regulacji prawnych chroniących dane osobowe. W artykule omówiono najważniejsze aspekty Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Rozporządzenie ma obowiązywać w krajach UE od stycznia 2016 roku i wprowadza istotne zmiany szczególnie w aspekcie ochrony danych osobowych w tym danych dotyczących zdrowia